Amendment to the Drawings

Please substitute the enclosed drawing figures 1, 2 and 4 for the originally submitted figures. The only changes are that block 108 has been relabeled CA MANAGEMENT SYSTEM. A marked up version is enclosed to show the location of the correction.

REMARKS

This application has been carefully reviewed in view of the above-referenced Office Action in which new grounds for rejection have been presented. Reconsideration is requested in view of the following remarks.

Overview Of the Technology

In order to understand the distinctions between the presently claimed invention and the cited references, it is useful to review an embodiment of the invention and the cited art. It is noted that the language of the claims as presented may be somewhat ambiguous and inconsistent with the language used in the specification, creating an opportunity for the claim language to be interpreted in an unintended manner. Applicant regrets this apparent inconsistency, and wishes to clarify the language of the claims and specification by this amendment.

The noted inconsistency is that the specification refers to block 108 as a CA system throughout. However, it will be clear that block 108 should more properly be referred to as a conditional access management system (as used in the claims) which forms only a portion of the whole CA system itself. Applicant has also amended the specification and drawings to use more appropriate naming of block 108. Its functionality is as described, and will be clear to those skilled in the art. The CA management system 108 operates in the manner described by use of the subscriber 114 database to track the authorization status of subscribers to the various available content. The CA management system 108 interacts with the content encryption block 104 to provide for addressing of content to subscribers and management of encryption keys. The above-noted errors are in naming alone, and do not impact the teachings of the specification. As a result of this minor error, the undersigned understands how the claims can be misinterpreted and wishes to clarify the record accordingly. The language used in connection with this technology is not fully standardized, so it is imperative that a proper consideration of the teachings of the specification be taken into consideration.

In accordance with embodiments of the invention, a conditional access management (CAM) system (108) and conditional access encryption system (CAE) (encryption block 104) system are both at the cable or service provider head end (which could be centralized or

distributed, but in any event is upstream from the receiver STB (page 2, lines 13-17). The basic problem being addressed is that if a portion of the system must reboot, or if communication is otherwise lost between components of the CA system at the transmitter side, it is possible (and indeed it has happened in the field) that content that should be transmitted as encrypted content could be transmitted in the clear so that it is available for all to view. This is a serious problem for at least three reasons: 1) digital copyrighted content could be made available without protection enabling easy pirating, 2) unauthorized subscribers could receive the content without paying for it, and 3) content which is unsuitable for consumption by children (e.g., adult movies and the like) would be transmitted in the clear and hence be viewable by children. Of course, the third reason may be the most compelling since it is highly undesirable for adult movies and the like to be available to children. Further, it is more desirable that content be inaccessible to authorized subscribers than for the content to be exposed to unauthorized subscribers such as children. To complicate matters, in certain real world systems, the situation can go unnoticed for many hours – resulting in the above undesirable situation to exist unchecked for quite some time.

The problem is addressed in certain embodiments of the invention by always assuring that some form of encryption is being used for content that is intended to be encrypted. In the present case, a default encryption key is used if there is any loss in communication between any of the various components of the conditional access system which control such encryption and CA functions.

Regarding the cited art in general

The Maillard reference of record describes a conditional access system that uses smart cards at the receiver for decryption functions. As is apparently acknowledged by the Examiner, Maillard does not disclose encrypting certain content using a default key in the event of a communication failure (see paragraph spanning pages 3 and 4). The Office seems to assert that Maillard discloses a default encryption mechanism, but the undersigned is unable to find any such disclosure.

The Bestler reference of record, as understood, describes use of session data packets that are alternately encrypted/decrypted with two different session keys (col.3, lines 1-6). When a

new key (a third key) is provided by the headend, one of the old keys continues to work for a time, while the other is rendered obsolete. New keys can thereby be introduced periodically as desired to enhance the system's security (col. 5, lines 19-22). Unauthorized users having only the obsolete key cannot decrypt the content once a polling cycle and key distribution cycle is complete (col. 5, lines 36-59). A default key is discussed with reference to U.S. Patent no. 4,771,458. Reference to this patent indicates that the default key is used only for decryption of global data, not for addressed data "One of the global decryption keys is a permanent default key associated with the subscriber terminal to assure that communication with that terminal is possible despite a lack of knowledge of the terminal address or the other global decryption keys in its memory." (abstract) Thus, essentially, the default key is a key of last resort for communication of data between the headend and the subscriber terminal. There is no teaching or suggestion of use of this default key for communication of A/V content.

Regarding the Rejections under 35 U.S.C. §103

Claims 1-40 were rejected on the combination of Maillard and Bestler of record.

First consider independent claim 1. In order to establish *prima facie* obviousness, the Office Action must establish the presence of each claim feature of in the cited art and provide articulated reasoning with rational underpinning for the obviousness of the combination of claim features and their interrelationship. In the present case, when either the original language of the claims or the amended language of the claims is considered, there is no teaching or suggestion (or articulated explanation for the absence of) anything in the combination of references that would lead one of ordinary skill in the art to "to encrypt certain audio/video content upon a communication failure between the conditional access encryption system and the conditional access management system" as required by independent claim 1.

The Office Action asserts that this teaching is found at col. 3, lines 1-6, col 5, lines 19-22, col. 5, lines 37-39 and col. 5, lines 60-63 of Bestler. However, upon review of these passages and the entire specification, including the referenced patent number 4,771,458, the undersigned is unable to find any discussion of procedures that are carried out in the event of a

communication failure. At most, there is a discussion that for global data packets*, the subscriber device tries each of the three available session keys including a default key, to attempt to decrypt global data packets; and, that the alternating key system can be used to update session keys. To even further distinguish over this aspect of Bestler, claim 1 has been amended to assure that the decrypted content in question is audio/video content (meaning packets containing audio and/or video content as contrasted with "global data packets"). Recall that Bestler discloses that the default key is used for decryption of the global data packets, not A/V content. Reconsideration and allowance of claim 1 and all claims dependent thereon are hereby respectfully requested.

Regarding independent claim 9, this claim calls for a similar feature of "means for storing default encryption information for the conditional access system for use by the conditional access system to encrypt certain audio/video content upon a communication failure between a portion of the conditional access system and the conditional access management system". The Office Action is deficient in rejection of this claim for similar reasons to that described in connection with claim 1. This claim has also been amended to clarify that the content is audio/video content, but this clarification is not necessary to overcome the cited reference. Reconsideration and allowance of claim 9 and all claims dependent thereon are hereby respectfully requested.

Regarding independent claims 16, 23, 29 and 35, these claims call for a set of actions that occur "if a communication failure occurs between the conditional access management system and the conditional access system". The Office Action is deficient in rejection of this claim for similar reasons to that described in connection with claim 1. It is noted that these claims are also amended to clarify that the content is audio/video content, but this amendment is not necessary to overcome the cited reference. Reconsideration and allowance of claims 16, 23, 29 and 35 and all claims dependent thereon are hereby respectfully requested.

---

* "The global packet is used for conveying program identification "tags" for special programs, such as movie channels, and for controlling subscriber terminal decoders for pay-per-view programming." See col. 1, line 67-col. 2, line 3; col. 3, line 58-64 of 4,771,458, which is referenced by Maillard, for example.

While other distinctions are present in the claims, these need not be addressed at this time. In view of the above remarks, reconsideration and allowance of claims 1-40 are respectfully requested.

Regarding the Rejections under 35 U.S.C. §102

Claims 41-57 were rejected based upon the Maillard reference of record.

Maillard is asserted to teach all aspects of these claims, but the Office Action references only segments of the Maillard reference that makes broad general statements regarding the various hardware configurations used in Maillard, and one reference to the system which "is able to emit accurate messages when an error occurs in a message". These teachings clearly fail to rise to the level of teaching to anticipate or enable the invention as claimed in claims 41-57. That notwithstanding, it is appreciated that the claims as presently drafted are subject to broad interpretation. Therefore, the claims have been amended to assure greater clarity and to assure that the cited art is more clearly inapplicable. Reconsideration and allowance of claims 41-57 are respectfully requested.

Concluding Remarks

The undersigned additionally notes that many other distinctions exist between the cited art and the claims. However, in view of the clear distinctions pointed out above, it is submitted that further discussion is unnecessary. No amendment made herein was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim unless an argument has been made herein that such amendment has been made to distinguish over a particular reference or combination of references.

Interview Request

In view of this communication, all claims are now believed to be in condition for allowance and such is respectfully requested at an early date. If further matters remain to be resolved, the undersigned respectfully requests the courtesy of an interview. The undersigned

can be reached at the telephone number below.

Respectfully submitted,

/Jerry A. Miller 30779/

Jerry A. Miller
Registration No. 30,779

Dated: 3/10/2008

Please Send Correspondence to:
Miller Patent Services
2500 Dockery Lane
Raleigh, NC 27606
Phone: (919) 816-9981
Fax: (919) 816-9982
Customer Number 24337